

## Distributed telematic system management method

Patent Number: FR2750275

Publication date: 1997-12-26

Inventor(s): CHOMEL BRUNO; MICHON PHILIPPE; PETIT STEPHANE

Applicant(s): FRANCE TELECOM (FR)

Requested Patent:  FR2750275

Application Number: FR19960007763 19960621

Priority Number(s): FR19960007763 19960621

IPC Classification: H04L9/32

EC Classification: G07F7/08C6, G07F17/16, G07F19/00F6

Equivalents:

### Abstract

The method involves use of a user inquiry terminal (10) which sends a request to a prestation server (11) via an interface (12). The server then replies to the information request. A further request is then sent to the user inquiry terminal for payment. The inquiry terminal can then complete the transaction, allowing the user to purchase goods. A request is then sent to an acquisition system (20) to order the goods.

Data supplied from the esp@cenet database - I2

(19) RÉPUBLIQUE FRANÇAISE  
INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE  
PARIS

(11) N° de publication : 2 750 275  
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : 96 07763

(51) Int Cl<sup>6</sup> : H 04 L 9/32

(12)

## DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 21.06.96.

(30) Priorité :

(71) Demandeur(s) : FRANCE TELECOM  
ETABLISSEMENT PUBLIC — FR.

(43) Date de la mise à disposition du public de la demande : 26.12.97 Bulletin 97/52.

(56) Liste des documents cités dans le rapport de recherche préliminaire : Se reporter à la fin du présent fascicule.

(60) Références à d'autres documents nationaux apparentés :

(72) Inventeur(s) : CHOMEL BRUNO, MICHON PHILIPPE et PETIT STEPHANE.

(73) Titulaire(s) : ..

(74) Mandataire : SOCIETE DE PROTECTION DES INVENTIONS.

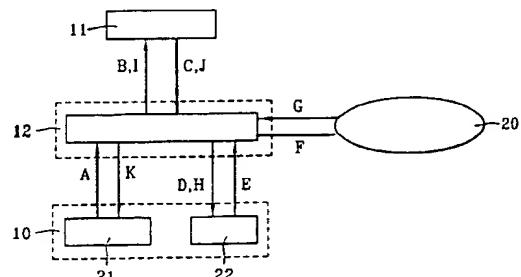
### (54) PROCÉDÉ DE GESTION DANS UN SYSTÈME TELEMATIQUE DISTRIBUÉ ET SYSTÈME DE MISE EN OEUVRE DE CE PROCÉDÉ.

(57) La présente invention concerne un procédé de gestion dans un système télématique distribué comprenant:

- un terminal de consultation;
- au moins un serveur de prestations;
- un frontal de communication;
- au moins un système acquéreur.

Ledit procédé comprend les différentes étapes suivantes, vues du frontal de communication:

- réception d'une demande de prestation (A) en provenance du terminal de consultation;
- envoi d'une demande d'informations (B) à un serveur de prestations;
- réception d'informations (C) en provenance de ce serveur de prestations;
- envoi d'une requête (D) au terminal de consultation;
- réception d'une transaction (E) en provenance du terminal de consultation;
- soumission de cette transaction (F) à un système acquéreur;
- réception d'un acquittement (G) en provenance de ce système acquéreur;
- envoi de cet acquittement (H) au terminal de consultation.



FR 2 750 275 - A1



PROCEDE DE GESTION DANS UN SYSTEME TELEMATIQUE  
DISTRIBUE ET SYSTEME DE MISE EN OEUVRE DE CE PROCEDE

DESCRIPTION

5

Domaine technique

La présente invention concerne un procédé de gestion dans un système télématique distribué et un système de mise en oeuvre de ce procédé.

Etat de la technique antérieure

Un système télématique distribué simple, comme illustré sur la figure 1, comporte trois types d'entités :

- un terminal de consultation 10, distant ou non, sur lequel l'utilisateur consulte, à titre onéreux ou non, des informations ;
- un serveur de prestations 11, distant ou non, qui fournit les informations consultées sur le terminal de consultation ;
- un frontal de communication 12 qui met en relation le terminal de consultation et le serveur de prestations.

Lorsque les informations sont consultables à titre onéreux, il est indispensable de disposer de mécanismes permettant de réaliser le paiement effectif de ces informations.

Dans les systèmes télématiques distribués, les systèmes de paiement utilisés pour réaliser le paiement des informations télématiques sont très limités.

Ainsi dans un système de kiosque à la durée, comme illustré sur la figure 2, le frontal de communication compte le temps alloué à une communication télématiche, calcule la consommation au prorata du temps passé pendant la communication télématiche et impute cette consommation sur le compte de l'utilisateur, qu'il a identifié au préalable, de la communication télématiche. Dans un tel système le coût de la communication télématiche (la consommation) ne dépend pas de la qualité des informations échangées lors de la communication télématiche.

Dans une procédure liée à un moyen de paiement bancaire, par exemple une carte bancaire avec une procédure dite VPC (vente par correspondance), le numéro de la carte bancaire est transmis pendant la communication télématiche au prestataire gérant le serveur de prestations. Ce numéro est utilisé pour compléter une transaction monétique comprenant des informations telles que le montant de la prestation télématiche, des données liées au prestataire gérant le serveur de prestations et des données liées au contexte de l'opération (date et heure notamment). Cette transaction monétique est, par la suite, présentée par le prestataire gérant le serveur de prestations au système bancaire pour paiement effectif. Cette procédure permet le paiement des informations à leur prix effectif. Elle ne nécessite que peu d'outils techniques pour être mise en oeuvre (une simple saisie est suffisante) mais elle présente les défauts de ne pas être garantie par le système bancaire et d'être peu sécurisée.

Dans une procédure sécurisée liée à un moyen de paiement bancaire, comme illustré sur la

figure 3, par exemple une carte bancaire utilisée en procédure de télépaiement sécurisée telle que celle-ci a été définie par le GIE cartes bancaires dans le « manuel du télépaiement sécurisé par carte bancaire » (une telle procédure est utilisée dans le cadre du système Facitel sur le réseau Télétel), après l'établissement d'un devis entre le prestataire de service et l'utilisateur, on reroute celui-ci vers un serveur 13 dédié au paiement par carte bancaire. Ce serveur dit « de paiement » pilote alors le terminal de l'utilisateur pour élaborer la transaction carte bancaire, effectue les vérifications réglementaires (vérification du certificat carte bancaire, vérification de la cohérence des informations inscrites sur la carte bancaire, ...) et renvoie au prestataire de service dans le message de reroutage arrière un acquittement (comprenant en partie la transaction monétique réalisée) positif ou négatif. Cet acquittement est aussi envoyé une seconde fois de façon « off-line » au prestataire de service qui effectue lui-même la remise de la transaction monétique auprès des systèmes bancaires acquéreurs. Sur la figure 3 est représenté un lecteur 14 de carte bancaire 15.

L'objet de la présente invention est de proposer un système télématique distribué et un ensemble d'échanges établis entre toutes les entités de ce système permettant de réaliser des opérations de paiement à distance liées à l'achat des biens électroniques ou non, transitant ou non par le réseau télématique du système télématique distribué.

Exposé de l'invention

La présente invention propose un procédé de gestion dans un système télématique distribué 5 comprenant :

- un terminal de consultation ;
  - au moins un serveur de prestations ;
  - un frontal de communication ;
  - au moins un système acquéreur ;
- 10 caractérisé en ce que ledit procédé comprend les différentes étapes suivantes, vues du frontal de communication ;
- réception d'une demande de prestation en provenance du terminal de consultation ;
- 15 - envoi d'une demande d'informations à un serveur de prestations ;
- réception de ces informations en provenance de ce serveur de prestations ;
  - envoi d'une requête au terminal de 20 consultation ;
  - réception d'une transaction en provenance du terminal de consultation ;
  - soumission de cette transaction à un système acquéreur ;
- 25 - réception d'un acquittement en provenance de ce système acquéreur ;
- envoi de cet acquittement au terminal de consultation.

30 Dans un premier mode de réalisation si cet acquittement est positif, on a également :

- envoi d'une demande de ladite prestation au serveur de prestations ;
- réception de ladite prestation en 35 provenance du serveur de prestations ;

- envoi de ladite prestation au terminal de consultation.

Dans un second mode de réalisation l'étape 5 de réception des informations en provenance du serveur de prestations comporte également une réception de la prestation en provenance dudit serveur limitant en cas d'acquittement positif les échanges au seul envoi de ladite prestation au terminal de consultation.

10

Avantageusement le terminal de consultation a un dispositif payeur ayant les fonctionnalités suivantes :

- l'utilisateur choisit localement (au 15 moment où il le désire) son plan de paiement, dans les limites réglementaires acceptées par les différents systèmes acquéreurs ;

- l'utilisateur configure le dispositif payeur du terminal de consultation sur les seuils de 20 confirmations explicites ou implicites qu'il désire mettre en place suivant les moyens de paiement utilisés et la réglementation attenant à ces moyens ;

- le dispositif payeur du terminal de consultation peut afficher le cumul des consommations 25 de la pseudo-session en cours, soit globalement, soit de façon détaillée pour chaque moyen de paiement utilisé par l'utilisateur ;

- le dispositif payeur du terminal de consultation peut gérer plusieurs utilisateurs ayant 30 chacun un plan de paiement et des moyens de paiement à disposition ;

- le dispositif payeur du terminal de consultation intègre le traitement de messages dits de service qui permettent notamment la réalisation de 35 l'identification/authentification de l'utilisateur vis-

à-vis du système télématique distribué et la gestion des fonctionnalités de traitement des litiges ;

5 - le dispositif payeur du terminal de consultation dispose d'un système permettant de gérer, notamment dans le cas d'utilisation de la technologie Porte-Monnaie Virtuel, des clés secrètes liées aux divers utilisateurs du dispositif payeur du terminal de consultation.

10 Avantageusement avec un système acquéreur de type Porte-Monnaie Virtuel, on a les étapes suivantes :

15 - à la requête de paiement, le module du dispositif payeur du terminal de consultation de l'utilisateur, traitant le Porte-Monnaie Virtuel, réalise une signature électronique sur les éléments de la requête pour élaborer la transaction monétique, cette signature électronique étant réalisée à l'aide d'un algorithme à clé publique et de la clé secrète de 20 l'utilisateur ;

- la transaction ainsi réalisée, après avoir transité par le frontal de communication est présentée au système acquéreur Porte-Monnaie Virtuel ;

25 - le système acquéreur Porte-Monnaie Virtuel s'assure alors de la validité de la transaction présentée, en vérifiant notamment la signature électronique à l'aide de la clé publique de l'utilisateur et le solde du compte de l'utilisateur, puis impute sur le compte de l'utilisateur le montant 30 de la transaction ;

35 - en réponse à la sollicitation du frontal de communication, présentation de la transaction et après traitement de la transaction, le système acquéreur Porte-Monnaie Virtuel renvoie un acquittement positif ou négatif.

à-vis du système télématique distribué et la gestion des fonctionnalités de traitement des litiges ;

5 - le dispositif payeur du terminal de consultation dispose d'un système permettant de gérer, notamment dans le cas d'utilisation de la technologie Porte-Monnaie Virtuel, des clés secrètes liées aux divers utilisateurs du dispositif payeur du terminal de consultation.

10 Avantageusement avec un système acquéreur de type Porte-Monnaie Virtuel, on a les étapes suivantes :

15 - à la requête de paiement, le module du dispositif payeur du terminal de consultation de l'utilisateur, traitant le Porte-Monnaie Virtuel, réalise une signature électronique sur les éléments de la requête pour élaborer la transaction monétique, cette signature électronique étant réalisée à l'aide d'un algorithme à clé publique et de la clé secrète de l'utilisateur ;

20 - la transaction ainsi réalisée, après avoir transité par le frontal de communication est présentée au système acquéreur Porte-Monnaie Virtuel ;

25 - le système acquéreur Porte-Monnaie Virtuel s'assure alors de la validité de la transaction présentée, en vérifiant notamment la signature électronique à l'aide de la clé publique de l'utilisateur et le solde du compte de l'utilisateur, puis impute sur le compte de l'utilisateur le montant de la transaction ;

30 - en réponse à la sollicitation du frontal de communication, présentation de la transaction et après traitement de la transaction, le système acquéreur Porte-Monnaie Virtuel renvoie un acquittement positif ou négatif.

Avantageusement on peut utiliser une clé secrète, liée à l'utilisateur du dispositif payeur du terminal de consultation, qui est stockée chiffrée sur son terminal, dans lequel pour pouvoir utiliser sa clé secrète l'utilisateur doit réaliser deux opérations :

- présenter son identifiant ; la présentation de cet identifiant permet de sélectionner une clé secrète chiffrée parmi plusieurs clés secrètes chiffrées ;
- 10 - présenter son code confidentiel (d'une longueur suffisante pour assurer la protection de la clé secrète) ; ce code confidentiel permet après traitement (fonction de hachage) de déchiffrer la clé secrète associée à l'identifiant de l'utilisateur.

15 Avantageusement avec un système acquéreur de type télépaiement sécurisé par carte bancaire, on a les étapes suivantes :

- à la requête de paiement, le module du dispositif payeur du terminal de consultation de l'utilisateur, traitant la carte bancaire, lit les informations liées au porteur de la carte bancaire (l'utilisateur ou non) et fait réaliser, par la carte bancaire, après saisie et présentation du code confidentiel, une signature électronique sur les éléments de la requête de paiement pour élaborer la transaction monétique, cette signature électronique étant réalisée à l'aide de l'algorithme présent dans la carte bancaire du porteur (l'utilisateur ou non) ;
- 20 - la transaction ainsi réalisée, après avoir transité par le frontal de communication est présentée au système acquéreur télépaiement sécurisé par carte bancaire ;
- 25 - le système acquéreur télépaiement sécurisé par carte bancaire s'assure alors de la

validité de la transaction présentée, en respectant les règles communément admises pour le traitement de la carte bancaire (conformément aux spécifications bancaires en vigueur) ;

5 - en réponse à la sollicitation du frontal de communication, présentation de la transaction et après traitement de la transaction, le système acquéreur télèpaient sécurisé par carte bancaire renvoie un acquittement positif ou négatif. Il conserve  
10 la transaction acquittée qu'il remet à échéance fixée par les systèmes bancaires au centre de télécollecte.

L'invention concerne également un système de mise en œuvre de ce procédé, caractérisé en ce  
15 qu'il comprend :

- un terminal de consultation comportant un dispositif client et un dispositif payeur ;  
- un serveur de prestations ;  
- un frontal de communication ;  
20 - au moins un système acquéreur dans lequel le terminal de consultation est relié logiquement au frontal de communication, le frontal de communication est relié au serveur de prestation, le frontal de communication est relié logiquement aux systèmes acquéreurs.  
25

Le dispositif client permet un envoi de requête au frontal de communication et le traitement des réponses associées.

30 Le dispositif payeur permet au terminal de consultation de recevoir les sollicitations de la part du frontal de communication, sollicitations qui suscitent ou non de sa part des réponses.

Le dispositif payeur peut également permettre de réaliser des opérations liées à l'identification/authentification de l'utilisateur.

5 Le dispositif payeur peut également permettre de réaliser des opérations liées aux services de paiement telles que le paiement de facture, le rechargement de compte déporté, prépayé ou non.

10 Le procédé de gestion dans un système télématique distribué selon l'invention permet de réaliser des opérations de paiement à distance liées à l'achat des biens électroniques ou non, transitant ou non par le réseau télématique du système télématique distribué.

15 Il peut trouver, notamment, une application dans les systèmes nécessitant un paiement à la durée ou à l'acte.

#### Brève description des figures

- 20 - Les figures 1, 2 et 3 illustrent différents systèmes de l'art antérieur ;  
- les figures 4 et 5 illustrent un système permettant la mise en oeuvre du procédé de l'invention ;  
25 - la figure 6 illustre les différentes étapes du procédé de l'invention ;  
- la figure 7 illustre les différentes étapes d'une variante du procédé de l'invention ;  
- la figure 8 illustre schématiquement le fonctionnement du dispositif payeur du terminal de consultation ;  
30 - la figure 9 illustre l'utilisation d'une clé secrète liée à un utilisateur du dispositif payeur du terminal de consultation.

Exposé détaillé de modes de réalisation

Dans le système permettant de mettre en oeuvre le procédé de l'invention, comme illustré sur 5 les figures 4 et 5, le schéma de la figure 5 étant une simplification du schéma de la figure 4, on retrouve, comme dans un système télématico distribué simple, les entités suivantes :

10 - un terminal de consultation 10, distant ou non, sur lequel l'utilisateur consulte à titre onéreux ou non des informations ;

- un serveur de prestations 11, distant ou non, qui fournit les informations consultées sur le terminal de consultation ;

15 - un frontal de communication 12, qui met en relation le terminal de consultation et le serveur d'informations ; et

20 - des entités 20 ayant pour rôle l'acquisition et le traitement des transactions, par exemple de type monétique ; ces entités peuvent être de type communautaire (bancaire notamment) et/ou de type privé (paiement sur compte d'abonné par exemple) ; ces entités sont dénommées dans la suite « systèmes acquéreurs ».

25 Comme représenté sur la figure 4, on peut retrouver le lecteur 14 de carte 15 de la figure 3.

Toutes ces entités sont connectées logiquement entre elles de la façon suivante :

30 • Le terminal de consultation 10 est relié logiquement au frontal de communication 12. Ce terminal de consultation 10 comporte deux dispositifs. Le premier de ces dispositifs est un dispositif client 21 qui permet un envoi de requête au frontal de communication 12 et le traitement des réponses  
35

associées. Ce premier dispositif est dédié à la consultation des informations. Le second de ces dispositifs est un dispositif payeur 22 qui permet au terminal de consultation de recevoir des sollicitations 5 de la part du frontal de communication, sollicitations qui suscitent de sa part des réponses ou non. Ce second dispositif est dédié au traitement des opérations de paiement et au traitement d'opérations dites de service pour le système télématique (dont l'authentification de 10 l'utilisateur).

• Le frontal de communication 12 est relié logiquement aux serveurs de prestations. Chaque requête du terminal de consultation 10 peut être analysée par 15 le frontal de communication 12 et est transmise au serveur de prestations concerné. La réponse du serveur de prestations 11 peut être analysée par le frontal de communication et est retransmise au dispositif client du terminal de consultation.

20 • le frontal de communication 12 est relié logiquement aux systèmes acquéreurs 20. Le frontal de communication 12 présente au système acquéreur 20 adapté la transaction monétique issue du dispositif payeur du terminal de consultation. Le système acquéreur 20 répond à cette sollicitation par un acquittement qui peut être positif ou négatif.

30 Dans le procédé selon l'invention on a ainsi les différents échanges suivants, vus du frontal de communication 12 :

• Réception d'une demande de prestation (échange A) :

Le dispositif client 21 du terminal de consultation 10 demande une prestation par action de l'utilisateur. Cette demande de prestation est transmise au frontal de communication 12.

5

- Envoi d'une demande d'information, par exemple de devis (échange B) :

Le frontal de communication 12, pour la prestation demandée, effectue une demande 10 d'informations (devis) au serveur de prestations concerné 11.

- Réception d'informations (échange C) :

Le serveur de prestations 11 envoie au 15 frontal de communication 12 en réponse à sa demande d'informations, les informations (devis) qui comprennent des informations statiques décrivant les éléments invariants de la prestation (désignation de la prestation, ...), des informations variables décrivant 20 les éléments variables de la prestation (prix, disponibilité, ...) et des informations variables, par exemple liées au devis lui-même (validité du devis, ...).

25

- Envoi d'une requête, par exemple de paiement (échange D) :

A la réception de ces informations émises par le serveur de prestations 11, le frontal de communication 12 émet à destination du dispositif payeur 22 du terminal de consultation 10 une requête de paiement reprenant tout ou partie des informations (devis) émises par le serveur de prestations 11.

35 ◦ Réception d'une transaction, par exemple monétique (échange E) :

Le dispositif payeur 22 du terminal de consultation 10 élabore à l'aide du moyen de paiement choisi par l'utilisateur une transaction, par exemple monétique. Cette transaction comprend toutes les 5 informations nécessaires pour imputer le montant de la prestation sur le système gérant le moyen de paiement choisi par l'utilisateur. Cette transaction est envoyée en réponse au frontal de communication par le dispositif payeur 22 du terminal de consultation 10.

10

- Soumission de cette transaction (échange F) :

Le frontal de communication 12, à la réception de la transaction, ne sachant pas la traiter, 15 présente cette transaction au système acquéreur 20 adapté (interne ou externe) à cette transaction.

20

- Réception d'un acquittement, par exemple monétique (échange G) :

25

le système acquéreur 20 traite la transaction et renvoie au frontal de communication 12 un acquittement sur la transaction positif (acceptation de la transaction) ou négatif (refus de la transaction), suivant les critères exigés pour le traitement du moyen de paiement concerné.

35

- Envoi de cet acquittement (échange H) :

Le frontal de communication 12 renvoie l'acquittement reçu au dispositif payeur 22 du terminal de consultation 10. Aucune réponse n'est attendue. Le frontal de communication 10 traite l'acquittement reçu. Si l'acquittement reçu est négatif, la demande de prestation n'aboutit pas ; le cycle de demande d'une prestation est stoppé.

- Envoi d'une demande de prestation (échange I) :

5 Si l'acquittement reçu par le frontal de communication 12 est positif, le frontal de communication 12 envoie au serveur de prestations 11 la demande de prestation correspondant à la transaction envoyée précédemment.

- Réception de la prestation (échange J) :

10 Le serveur de prestation 11 envoie en réponse à la demande de prestation la prestation au frontal de communication 12.

- Envoi de la prestation (échange K) :

15 Le frontal de communication 12 envoie en réponse à la demande de prestation, la prestation au dispositif payeur 22 du terminal de consultation 10. L'opération de demande (achat) à distance d'une prestation du serveur de prestations 11 est close. Une 20 nouvelle opération de demande de prestation auprès d'un serveur d'informations déroule à nouveau le présent procédé.

25 Dans une première variante de réalisation, de façon à réduire le nombre d'échanges réalisés entre les diverses entités, le frontal de communication 12 reçoit après une « demande d'informations » (échange B figure 6) lesdites informations et la prestation. Cette prestation est alors stockée temporairement sur le 30 frontal de communication 12 qui la présente au dispositif client 21 du terminal de consultation 10 après l'acceptation de la transaction. Dans ce cas, les mouvements « Envoi d'une demande de prestation » (échange I figure 6) et « Réception de la prestation »

(échange J, figure 6) sont inexistant, comme illustré sur la figure 7.

Dans une seconde variante de réalisation, le dispositif payeur 22 du terminal de consultation 10 5 est dédié à d'autres opérations que celle du paiement des prestations des serveurs de prestations 11. Ainsi, on peut réaliser des opérations liées à l'identification/authentification de l'utilisateur. De même, on peut réaliser des opérations liées aux 10 services de paiement telles que le paiement de facture, le rechargement de compte déporté, prépayé ou non.

On va ci-dessous donner une description détaillée des fonctionnalités supportées par les 15 diverses entités du système, en reprenant chaque entité, et en décrivant précisément le rôle et les opérations qu'elles doivent assurer.

Dans la suite on considère à titre d'exemple une opération d'achat à distance d'une 20 prestation.

#### *Serveur de prestations 11*

25 Les serveurs de prestations doivent être capables de fournir un devis sur les prestations demandées et livrer les prestations demandées.

#### *Systèmes acquéreurs 20*

Divers systèmes acquéreurs permettant de réaliser le paiement peuvent être intégrés dans une telle architecture. Leur principe de fonctionnement 35 reste toujours le même. Ces systèmes répondent à une

sollicitation du frontal de communication, après traitement de la transaction avec les règles communément admises pour le moyen de paiement concerné, par un acquittement positif ou négatif. Pour illustrer 5 ce mode de fonctionnement, deux systèmes acquéreurs sont décrits par la suite. Ces deux systèmes ne présagent en rien les systèmes acquéreurs qui pourraient à terme être intégrés dans l'architecture du système télématicque distribué.

10

o Système acquéreur : « Porte-Monnaie Virtuel »

Le système acquéreur « Porte-Monnaie Virtuel » est fondé sur la gestion de comptes anonymes 15 ou non, que l'on débite et/ou crédite à l'aide d'algorithme à clé publique. Il fonctionne en complément du dispositif payeur du terminal de consultation de l'utilisateur. Le principe de fonctionnement d'un tel système de paiement est le 20 suivant :

\* A la requête de paiement, le module du dispositif payeur du terminal de consultation de l'utilisateur, traitant le Porte-Monnaie Virtuel, réalise une signature électronique sur les éléments de 25 la requête de paiement pour élaborer la transaction monétique. Cette signature électronique est réalisée à l'aide d'un algorithme à clé publique et de la clé secrète de l'utilisateur.

30

\* La transaction ainsi réalisée, après avoir transité par le frontal de communication est présentée au système acquéreur Porte-Monnaie Virtuel.

\* Le système acquéreur Porte-Monnaie 35 Virtuel s'assure alors de la validité de la transaction

présentée, en vérifiant notamment la signature électronique à l'aide de la clé publique de l'utilisateur et le solde du compte de l'utilisateur, puis impute sur le compte de l'utilisateur le montant 5 de la transaction.

\* En réponse à la sollicitation du frontal de communication, présentation de la transaction et après traitement de la transaction, le 10 système acquéreur Porte-Monnaie Virtuel renvoie un acquittement monétique positif ou négatif.

L'utilisation d'un système à clé publique présente quelques avantages dont la non-répudiation et 15 le paiement incrémental.

Il y a non-répudiation puisqu'il n'y a aucun secret partagé, la clé secrète n'est possédée que par une seule entité, l'utilisateur.

Le paiement incrémental permet de limiter 20 les interactions entre le système acquéreur Porte-Monnaie Virtuel et le frontal de communication. A la première transaction, le frontal de communication peut obtenir, outre l'acquittement de cette première transaction, une provision de consommation et la clé publique associée à la clé secrète de l'utilisateur. 25 Ainsi, sans solliciter à chaque transaction le système acquéreur Porte-Monnaie Virtuel, le frontal de communication a les moyens de vérifier la cohérence des transactions (dont les signatures électroniques) 30 présentées par le dispositif payeur du terminal de consultation de l'utilisateur, ce à concurrence de la provision indiquée par le système acquéreur Porte-Monnaie Virtuel. En fin de session télématico (pseudo-session dans certains contextes télématiques) ou en cas 35 d'atteinte de la provision, toutes les transactions

sont envoyées au système acquéreur Porte-Monnaie Virtuel qui les acquitte.

o Système acquéreur : « Télépaiement  
5 Sécurisé par Carte Bancaire ».

Le système acquéreur « Télépaiement Sécurisé par Carte bancaire » est fondé en partie sur des règles émises par le milieu bancaire, notamment dans les manuels de « Télépaiement Sécurisé par Carte Bancaire » et de « Paiement Electronique par Carte Bancaire » édités par le GIE des Cartes Bancaires. Il fonctionne en complément du dispositif payeur du terminal de consultation de l'utilisateur. Le principe de fonctionnement d'un tel système de paiement est le suivant :

\* A la requête de paiement, le module du dispositif payeur du terminal de consultation de l'utilisateur, traitant la carte bancaire, lit les informations liées au porteur de la carte bancaire (l'utilisateur ou non) et fait réaliser par la carte bancaire après saisie et présentation du code confidentiel, une signature électronique sur les éléments de la requête de paiement pour élaborer la transaction monétique. Cette signature électronique est réalisée à l'aide de l'algorithme présent dans la carte bancaire du porteur (l'utilisateur ou non).

\* La transaction ainsi réalisée, après avoir transité par le frontal de communication, est présentée au système acquéreur télépaiement sécurisé par carte bancaire.

\* Le système acquéreur télépaiement sécurisé par carte bancaire s'assure alors de la validité de la transaction présentée, en respectant les

règles communément admises pour le traitement de la carte bancaire (conformément aux spécifications bancaires en vigueur).

5 \* En réponse à la sollicitation du frontal de communication, présentation de la transaction et après traitement de la transaction, le système acquéreur télépaientement sécurisé par carte bancaire renvoie un acquittement positif ou négatif. Il  
10 conserve la transaction acquittée qu'il remet à échéance fixée par les systèmes bancaires au centre de télécollecte.

15

#### *Frontal de communication 12*

Le frontal de communication a pour rôle de gérer la succession des échanges de façon à pouvoir livrer des prestations gratuites, et faire payer et  
20 livrer des prestations payantes pour le compte de tiers : les serveurs d'informations. Pour cela :

\* Il peut demander et obtenir des devis sur les prestations demandées auprès des serveurs de  
25 prestations.

\* Il envoie au dispositif payeur du terminal de consultation des requêtes de paiement conformes aux devis établis et obtient des transactions monétiques du dispositif payeur du terminal de consultation.

\* Il présente au système acquéreur lié au moyen de paiement choisi par l'utilisateur la

transaction et traite l'acquittement qu'il obtient en réponse.

Une variante de ce système consiste à faire livrer par une autre voie que le réseau télématiche la prestation demandée (cas typique de la livraison d'un bien physique).

De même, le frontal de communication dialogue avec le dispositif payeur du terminal de consultation pour réaliser des opérations de services telles que l'identification/authentification de l'utilisateur.

Le frontal de communication a donc un rôle de médiation, notamment financière, entre les serveurs d'informations et les utilisateurs employant les terminaux de consultation. C'est pourquoi, il peut être appelé « médiateur télématiche ».

#### *Terminal de consultation 10*

20

Le terminal de consultation comprend deux dispositifs : un dispositif client 21 qui lui permet de demander et de recevoir les prestations télématisques, et un dispositif payeur 22 qui lui permet de réaliser des opérations de paiement et des opérations dites de services comme l'identification et l'authentification de l'utilisateur.

• Terminal de consultation : dispositif de consultation 21.

Ce dispositif 21 peut être choisi indifféremment dans la gamme des produits présents sur le marché.

o Terminal de consultation : dispositif payeur 22 permettant de réaliser le paiement et des opérations de services.

Le dispositif payeur 22 du terminal de consultation répond aux sollicitations du frontal de communication, notamment aux requêtes de paiement. la figure 8 présente schématiquement le fonctionnement du dispositif payeur du terminal de consultation. D étant une requête de paiement, E une transaction monétique et H un acquittement monétique. Ses fonctionnalités sont les suivantes :

\* L'utilisateur choisit localement (au moment où il le désire) son plan de paiement, dans les limites réglementaires acceptées par les différents systèmes acquéreurs. Etablir son plan de paiement consiste à désigner les moyens de paiement que l'on va utiliser pour payer les prestations et à fixer les montants limites d'utilisation d'un moyen de paiement, ceci en respectant les règles d'utilisation attenant aux moyens de paiement concernés. Par exemple, l'utilisateur décide de payer avec son Porte-Monnaie Virtuel toutes les prestations dont le montant est inférieur à 100 francs, les autres étant payées avec sa carte bancaire.

\* L'utilisateur configure le dispositif payeur du terminal de consultation sur les seuils de confirmations explicites ou implicites qu'il désire mettre en place suivant les moyens de paiement utilisés et la réglementation attenant à ces moyens.

\* Le dispositif payeur du terminal de consultation peut afficher le cumul des consommations de la pseudo-session en cours, soit globalement, soit

de façon détaillée pour chaque moyen de paiement utilisé par l'utilisateur.

5 \* Le dispositif payeur du terminal de consultation peut gérer plusieurs utilisateurs ayant chacun un plan de paiement et des moyens de paiement à disposition.

10 \* Le dispositif payeur du terminal de consultation intègre le traitement de messages dits de service qui permettent notamment la réalisation de l'identification/authentification de l'utilisateur vis-à-vis du système télématiche distribué et la gestion des fonctionnalités de traitement des litiges.

15 \* Le dispositif payeur du terminal de consultation dispose d'un système permettant de gérer, notamment dans le cas d'utilisation de la technologie Porte-Monnaie Virtuel, des clés secrètes liées aux divers utilisateurs du dispositif payeur du terminal de consultation.

25 On va à présent donner une description détaillée du système de protection des clés secrètes liées aux divers utilisateurs du dispositif payeur du terminal de consultation.

30 La clé privée d'un utilisateur est stockée chiffrée sur son terminal. Pour pouvoir utiliser sa clé secrète, un utilisateur doit réaliser deux opérations :

- présenter son identifiant ; la présentation de cet identifiant permet de sélectionner une clé secrète chiffrée parmi plusieurs clés secrètes chiffrées ;

- présenter son code confidentiel (d'une longueur suffisante pour assurer la protection de la clé secrète) ; ce code confidentiel permet après traitement (fonction de hachage) de déchiffrer la clé secrète associée à l'identifiant de l'utilisateur.

La clé secrète peut alors être utilisée pour signer une transaction (utilisation Porte-Monnaie Virtuel) mais aussi pour assurer d'autres services (identification/authentification, gestion de litiges, ...). La figure 9 présente de façon synthétique les opérations effectuées pour réaliser un tel traitement.

REVENDICATIONS

1. Procédé de gestion dans un système télématique distribué comprenant :
  - 5 - un terminal de consultation (10) ;
  - au moins un serveur de prestations (11) ;
    - un frontal de communication (12) ;
    - au moins un système acquéreur (20) ;
- 10 caractérisé en ce que ledit procédé comprend les différentes étapes suivantes, vues du frontal de communication ;
  - réception d'une demande de prestation (A) en provenance du terminal de consultation ;
  - 15 - envoi d'une demande d'informations (B) à un serveur de prestations ;
    - réception d'informations (C) en provenance de ce serveur de prestations ;
    - envoi d'une requête (D) au terminal de consultation ;
      - réception d'une transaction (E) en provenance du terminal de consultation ;
      - soumission de cette transaction (F) à un système acquéreur ;
    - 20 - réception d'un acquittement (G) en provenance de ce système acquéreur ;
      - envoi de cet acquittement (H) au terminal de consultation.
  - 25 2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre, si cet acquittement est positif :
    - envoi d'une demande de ladite prestation (I) au serveur de prestations ;
    - réception de ladite prestation (J) en provenance du serveur de prestations ;

- envoi de ladite prestation (K) au terminal de consultation.

5 3. Procédé selon la revendication 1, caractérisé en ce que l'étape de réception des informations (C) en provenance du serveur de prestations comporte également une réception de la prestation en provenance dudit serveur.

10 4. Procédé selon la revendication 1, caractérisé en ce que le terminal de consultation a un dispositif payeur dans lequel l'utilisateur choisit localement, au moment où il le désire, son plan de paiement, dans les limites réglementaires acceptées par les différents systèmes acquéreurs.

15 5. Procédé selon la revendication 4, caractérisé en ce que l'utilisateur configure le dispositif payeur du terminal de consultation sur les seuils de confirmations explicites ou implicites qu'il désire mettre en place suivant les moyens de paiement utilisés et la réglementation attenant à ces moyens.

20 6. Procédé selon la revendication 4, caractérisé en ce que le dispositif payeur du terminal de consultation affiche le cumul des consommations de la pseudo-session en cours, soit globalement, soit de façon détaillée pour chaque moyen de paiement utilisé par l'utilisateur.

25 7. Procédé selon la revendication 4, caractérisé en ce que le dispositif payeur du terminal de consultation gère plusieurs utilisateurs ayant chacun un plan de paiement et des moyens de paiement à disposition.

30 8. Procédé selon la revendication 4, caractérisé en ce que le dispositif payeur du terminal de consultation intègre le traitement de messages dits de service qui permettent notamment la réalisation de l'identification/authentification de l'utilisateur vis-

à-vis du système télématique distribué et la gestion des fonctionnalités de traitement des litiges.

9. Procédé selon la revendication 4, caractérisé en ce que le dispositif payeur du terminal de consultation dispose d'un système permettant de gérer, notamment dans le cas d'utilisation de la technologie Porte-Monnaie Virtuel, des clés secrètes liées aux divers utilisateurs du dispositif payeur du terminal de consultation.

10 10. Procédé selon la revendication 1, caractérisé en ce qu'avec un système acquéreur de type Porte-Monnaie Virtuel, on a les étapes suivantes :

15 - à la requête de paiement, un module d'un dispositif payeur (22) du terminal de consultation (10) de l'utilisateur, traitant le Porte-Monnaie Virtuel, réalise une signature électronique sur les éléments de la requête de paiement pour élaborer la transaction monétique, cette signature électronique étant réalisée à l'aide d'un algorithme à clé publique 20 et de la clé secrète de l'utilisateur ;

- la transaction ainsi réalisée, après avoir transité par le frontal de communication (12) est présentée au système acquéreur ;

25 - le système acquéreur s'assure alors de la validité de la transaction présentée, en vérifiant notamment la signature électronique à l'aide de la clé publique de l'utilisateur et le solde du compte de l'utilisateur, puis impute sur le compte de l'utilisateur le montant de la transaction ;

30 - en réponse à la sollicitation du frontal de communication (12), présentation de la transaction et après traitement de la transaction, le système acquéreur renvoie un acquittement positif ou négatif.

11. Procédé selon la revendication 1, caractérisé en ce qu'avec un système acquéreur de type télépaiement sécurisé par carte bancaire, on a les étapes suivantes :

5 - à la requête de paiement un module d'un dispositif payeur du terminal de consultation de l'utilisateur, traitant la carte bancaire, lit les informations liées au porteur de la carte bancaire et fait réaliser, par la carte bancaire, après saisie et  
10 présentation du code confidentiel, une signature électronique sur les éléments de la requête de paiement pour élaborer la transaction monétique, cette signature électronique étant réalisée à l'aide de l'algorithme présent dans la carte bancaire dudit porteur ;

15 - la transaction ainsi réalisée, après avoir transité par le frontal de communication est présentée au système acquéreur ;

20 - le système acquéreur s'assure alors de la validité de la transaction présentée, en respectant les règles communément admises pour le traitement de la carte bancaire ;

25 - en réponse à la sollicitation du frontal de communication, présentation de la transaction et après traitement de la transaction, le système acquéreur renvoie un acquittement positif ou négatif ; il conserve la transaction acquittée qu'il remet à échéance fixée par les systèmes bancaires au centre de télécollecte.

30 12. Procédé selon la revendication 1, caractérisé en ce qu'on utilise une clé secrète, liée à l'utilisateur du dispositif payeur du terminal de consultation, qui est stockée chiffrée sur son terminal, dans lequel pour pouvoir utiliser sa clé secrète l'utilisateur réalise deux opérations :

- il présente son identifiant, la présentation de cet identifiant permettant de sélectionner une clé secrète chiffrée parmi plusieurs clés secrètes chiffrées ;

5 - il présente son code confidentiel; ce code confidentiel permettant après traitement de déchiffrer la clé secrète associée à l'identifiant de l'utilisateur.

10 13. Système de mise en oeuvre du procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend :

- un terminal de consultation (10), comportant un dispositif client (21) et un dispositif payeur (22) ;

15 - un frontal de communication (12) ;  
- au moins un système acquéreur dans lequel le terminal de consultation (10) est relié logiquement au frontal de communication (12), le frontal de communication (12) est relié au serveur de prestation, le frontal de communication (12) est relié logiquement aux systèmes acquéreurs (20).

20 14. Système selon la revendication 13, caractérisé en ce que le dispositif client (21) permet un envoi de requête au frontal de communication (12) et le traitement des réponses associées.

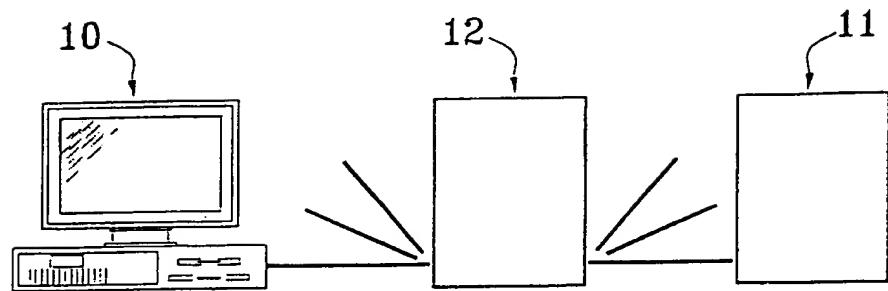
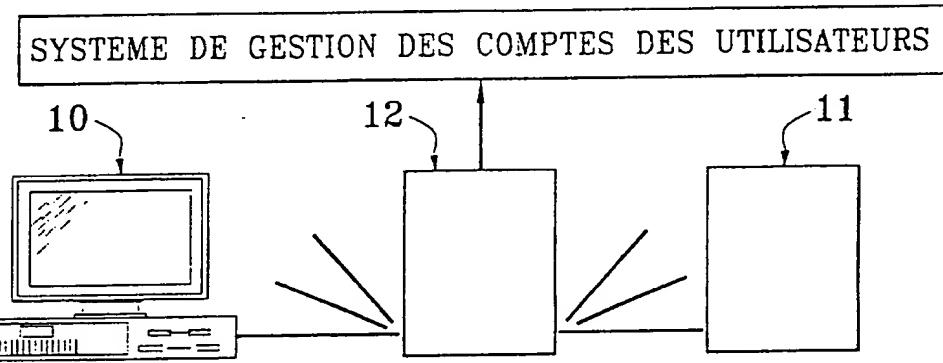
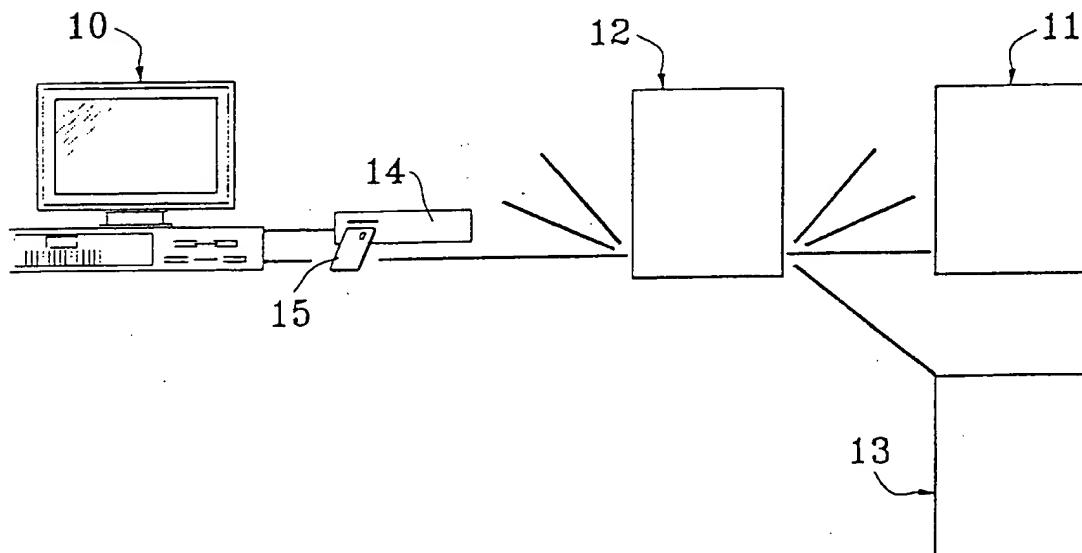
25 15. Système selon la revendication 13, caractérisé en ce que le dispositif payeur (22) permet au terminal de consultation (10) de recevoir les sollicitations de la part du frontal de communication (12), sollicitations qui suscitent ou non de sa part des réponses.

30 16. Système selon la revendication 13, caractérisé en ce que le dispositif payeur (22) permet de réaliser des opérations liées à l'identification/authentification de l'utilisateur.

17. Système selon la revendication 13, caractérisé en ce que le dispositif payeur (22) permet de réaliser des opérations liées aux services de paiement telles que le paiement de facture, le  
5 rechargement de compte déporté, prépayé ou non.

18. Système selon la revendication 13, caractérisé en ce que le dispositif payeur (22) répond aux sollicitations du frontal de communication, notamment aux requêtes de paiement ; l'utilisateur  
10 choisissant localement son plan de paiement dans les limites acceptées par les différents systèmes acquéreurs.

*1/4*  
*FIG. 1*

*FIG. 2**FIG. 3*

2/4

FIG. 4

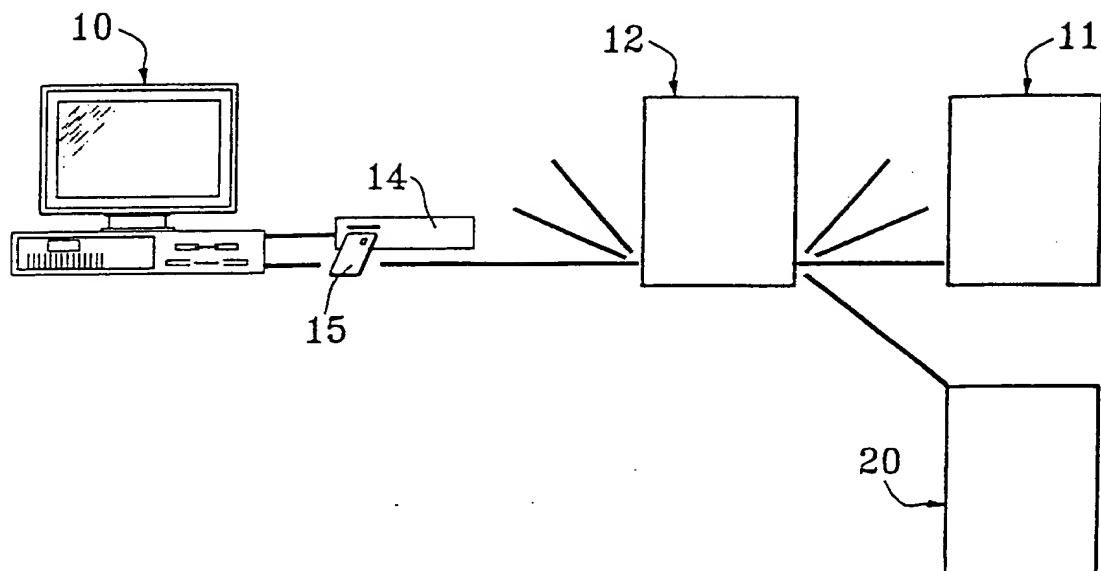
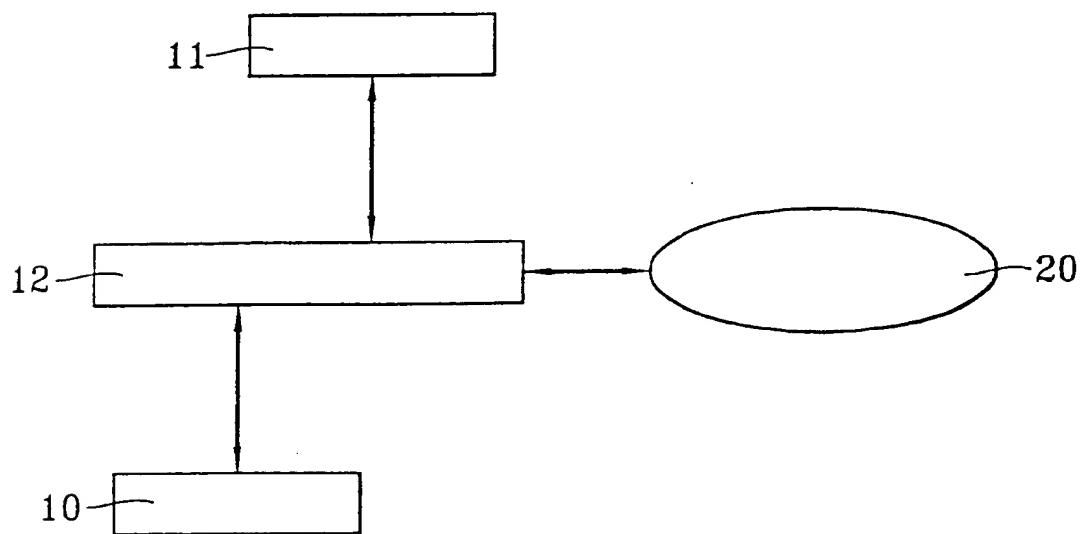


FIG. 5



3/4

FIG. 6

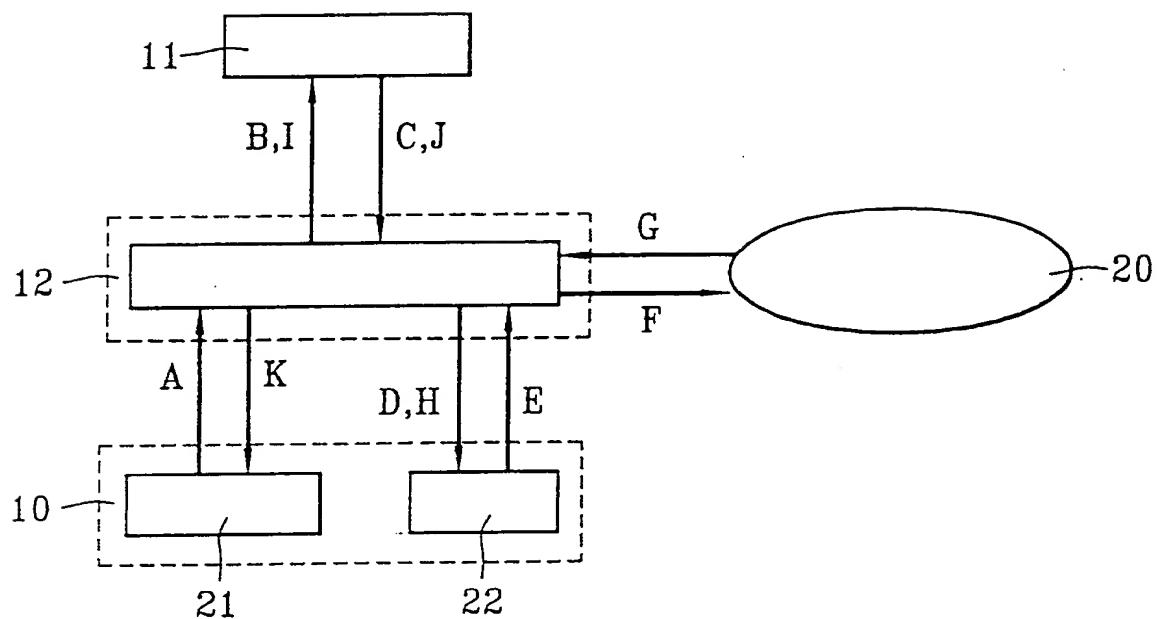
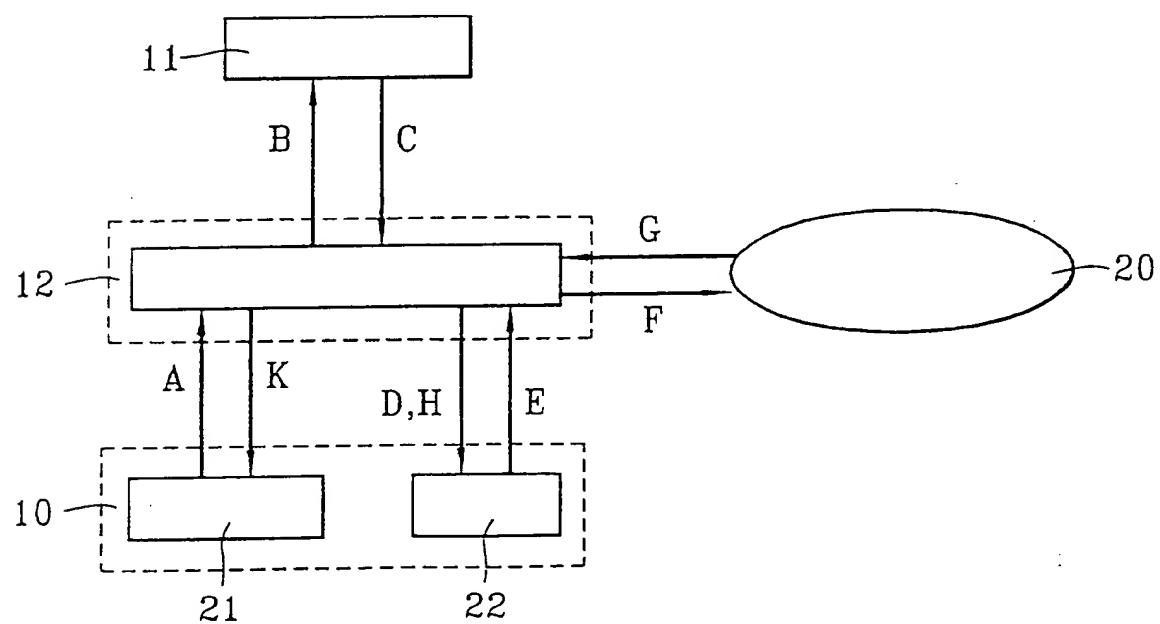


FIG. 7



4/4

FIG. 8

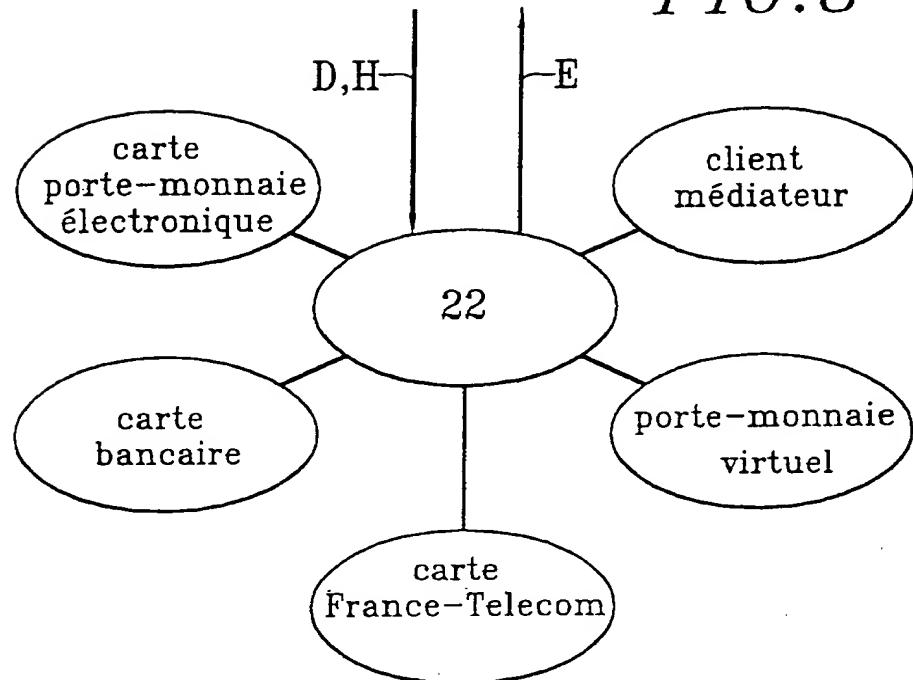
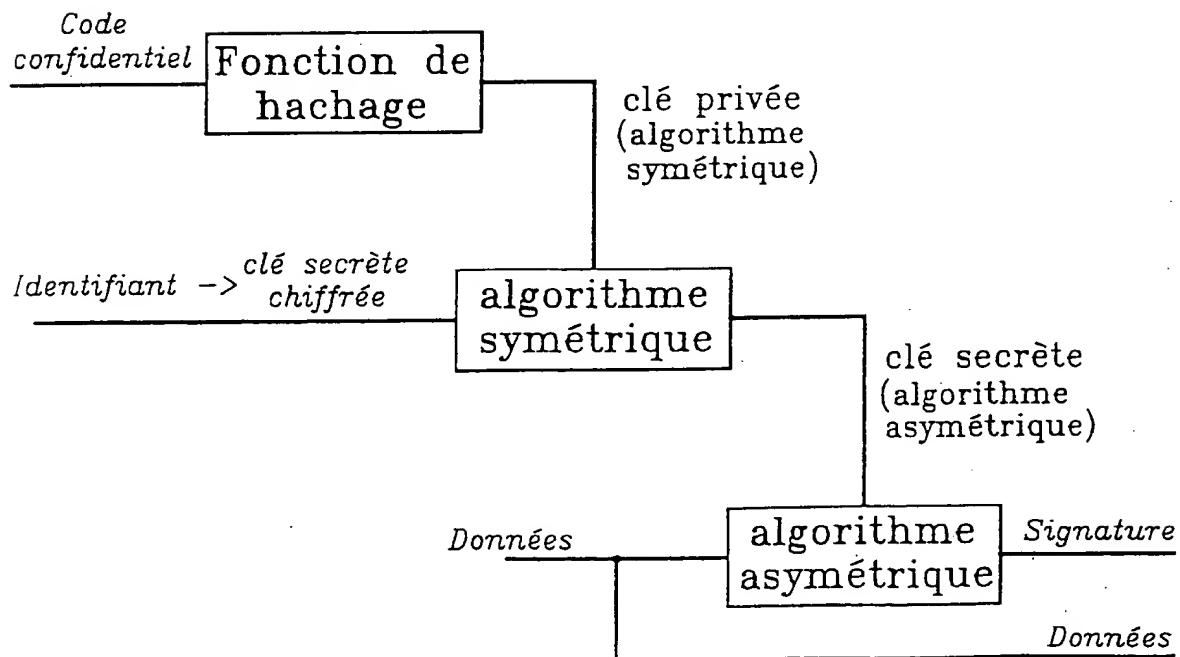


FIG. 9



REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL  
de la  
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE  
PRELIMINAIRE

établi sur la base des dernières revendications  
déposées avant le commencement de la recherche

2750275  
N° d'enregistrement  
national

FA 529219  
FR 9607763

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie		
Y	SIRBU M ET AL: "NETBILL: AN INTERNET COMMERCE SYSTEM OPTIMIZED FOR NETWORK DELIVERED SERVICES" 5 Mars 1995 , DIGEST OF PAPERS OF THE COMPUTER SOCIETY COMPUTER CONFERENCE (SPRING) COMPCON, TECHNOLOGIES FOR THE INFORMATION SUPERHIGHWAY SAN FRANCISCO, MAR. 5 - 9, 1995, NR. CONF. 40, PAGE(S) 20 - 25 , INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS XP000577034 * le document en entier * ---	1-3,8, 13-16
Y	EP 0 618 539 A (S.I. KIM )	1-3,8, 13-16
A	* abrégé; revendications; figures 1-3 *	11
A	EP 0 569 816 A (A. NOBUYUKI) * le document en entier *	1-4,7-9, 13-15,18
A	EP 0 542 298 A (CITIBANK) * abrégé; revendications; figures 1-10 *	1,4,9-11
A	EP 0 440 515 A (VISA) * abrégé; revendications; figures 1,3 *	1,4-8, 13,17,18
A	EP 0 494 530 A (STRATEGIC TELECOM) ---	G07F H04M
A	GIFFORD D K ET AL: "PAYMENT SWITCHES FOR OPEN NETWORKS" 5 Mars 1995 , DIGEST OF PAPERS OF THE COMPUTER SOCIETY COMPUTER CONFERENCE (SPRING) COMPCON, TECHNOLOGIES FOR THE INFORMATION SUPERHIGHWAY SAN FRANCISCO, MAR. 5 - 9, 1995, NR. CONF. 40, PAGE(S) 26 - 31 , INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS XP000577008 -----	DOMAINES TECHNIQUES RECHERCHES (Int.CL-6)
3	Date d'achèvement de la recherche	Examinateur
	22 Avril 1997	David, J
CATEGORIE DES DOCUMENTS CITES		T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons P : divulgation non-écrite O : membre de la même famille, document correspondant
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire		